eScholar Uniq-ID®
Administrator Guide: Security Management

Version 2020.3

Last Updated:

7.16.21

Bringing Data Together.

🔖 Getting Started

Chapter Highlights
- [Overview](#)
-

Overview

This Administrator Guide: Security Management can be used by administrators (Security Coordinators) to better understand how the security-related components work. The guide includes an overview of Security Manager which includes User Manager, Role Manager and the User Profile.

The guide includes this Getting Started chapter and is then split into a chapter per core feature. Each chapter will include a "Chapter Highlights" with bookmarks/links to the sub-sections within the chapter.

The guide will also include alerts/messages, including:

This indicator is used to highlight an important fact or detail about a feature or process.

This indicator is used to describe/define a specific term or reference that is used.

◼ Security Manager

Overview

The Security Manager feature enables authorized administrators to manage application roles and users. Access to this feature should be tightly controlled and limited to users with rights to add or edit users and edit roles. Changing settings in this component can impact data access and feature access.

Security Manager is divided into two core functions: User Manager and Role Manager. These functions are described in more detail below.

Security in the application is controlled by Authentication, Feature Authorization and Data Authorization, all of which are controlled within Security Manager.

Authentication

All users must have a registered and active account to log into DirectMatch. An authorized user must create the account and the user must complete the account set up process before the user can log in. DirectMatch utilizes an email address to uniquely identify a user. The email address is used as the username for the application.

Once an account is registered for a user, the user can log into the application with the URL. All users must authenticate to access the system.

Feature Authorization

The application has 18 roles available in the application and few of these roles are managed by district level users. Access to features and functions are controlled by these roles. Each role can be configured with permissions/privileges to features and functions as necessary by LDOE.

It is important to limit access to administrator level tasks to only the users that should be authorized to perform the task. For example, a School User should not be granted access to manage users with User Manager.

Data Authorization

Access to specific batches, transactions, and near matches is limited based upon assigned access to locations. A user must have access to a location to generate a match via Person ID, Upload File, or Individual Match, resolve a pending Near Match or to download data.

Security Manager

User Manager

User Manager (callout)

Role Manager (callout)

User Manager | | | | | **10** Users | **Add Records**

Filter Options ⌃

Email ⇕	First Name ⇕	Last Name ⇕	Status ⇕	Last Login ⇕	Role	Actions
ahartman@escholar.com	Andrea	Hartman	Active	05/28/2019	Location Administrator Super	🔑 »
nmoideen@escholar.com	Nishan	Moideen	Inactive	05/10/2019	Super	»
yzhang@escholar.com	Yuqing	Zhang	Pending		Help Desk	🗑 ✈ »
nmoideen@escholar.com	Nishan	Moideen	Active	05/10/2019	System Administrator	🔑 »
ahartman@escholar.com	Andrea	Hartman	Active	05/28/2019	Building Administrator	🔑 »
nmoideen@escholar.com	Nishan	Moideen	Active	05/10/2019	Building User	🔑 »
ahartman@escholar.com	Andrea	Hartman	Active	05/28/2019	Building User - DirectMatch	🔑 »
nmoideen@escholar.com	Nishan	Moideen	Active	05/10/2019	Location Administrator	🔑 »
ahartman@escholar.com	Andrea	Hartman	Active	05/28/2019	Super	🔑 »
nmoideen@escholar.com	Nishan	Moideen	Active	05/10/2019	Location Administrator - Location ID	🔑 »

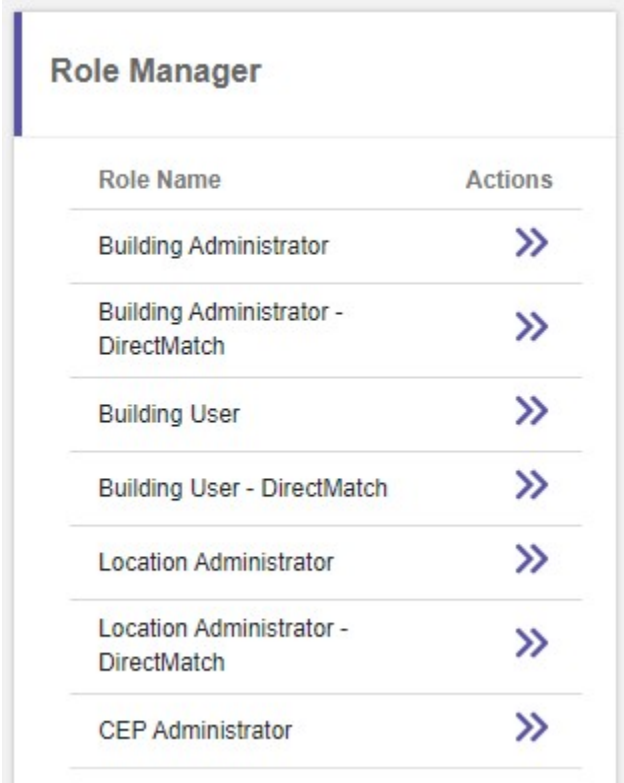1 - 10 of 10   Previous **1** Next

User Manager Actions (callout)

Role Manager Actions (callout)

Role Manager

Role Name	Actions
Building Administrator	»
Building Administrator - DirectMatch	»
Building User	»
Building User - DirectMatch	»
Help Desk	»
Location Administrator	»
Location Administrator - DirectMatch	»
Location Administrator - Location ID	»
Multiple Locations	»
Multiple Locations Specific Buildings	»
Search	»
Super	»

🔖 Security Manager - Role Manager

The Role Manager panel contains a list of roles that the user is authorized to access in the application. Users can only access roles below their own level and cannot edit roles above their own role. The Role Manager panel provides a list of each role and an action button to Drill into the Role Profile.

The application includes the following roles:

ROLE	DESCRIPTION	PARENT ROLE
Building Administrator	Typically reserved for users who require building/school level access to batches, transactions, and downloads. This role may have privileges that a Building User does	Location Administrator

ROLE	DESCRIPTION	PARENT ROLE
	not have. This role can view the Building Administrator and Building User roles only. This user role typically does not have access to Security Manager or Configuration Manager or other system administrator functions. Formerly named School Administrator.	
Building Administrator - DirectMatch	Typically reserved for users who require building/school level access to batches, transactions, and downloads in DirectMatch only. This role can view the Building Administrator – DirectMatch and Building User - DirectMatch roles only. This user role typically does not have access to Security Manager or Configuration Manager or other system administrator functions. Formerly named School Administrator - DirectMatch.	Location Administrator - DirectMatch
Building User	Typically reserved for users who require building/school level access to batches, transactions, and downloads. This role should not have access to Security Manager, but if enabled they would only see the Building User role.	Building Administrator

ROLE	DESCRIPTION	PARENT ROLE
	This user role typically does not have access to Security Manager or Configuration Manager or other system administrator functions. Formerly named School User.	
Building User – DirectMatch	Typically reserved for users who require building/school level access to batches, transactions, and downloads for DirectMatch. This role should not have access to Security Manager, but if enabled they would only see the Building User – DirectMatch role. This user role typically does not have access to Security Manager or Configuration Manager or other system administrator functions. Formerly named School User - DirectMatch.	Building Administrator - DirectMatch
Location Administrator	Typically reserved for users who require district and school level access to batches, transactions, and downloads. This role can view the Location Administrator, Building Administrator and Building User roles only. This user role typically does not have access to Configuration Manager or other	System Administrator

ROLE	DESCRIPTION	PARENT ROLE
	system administrator functions but may have access to User Manager. Formerly named District User (District Security Coordinator).	
Location Administrator - DirectMatch	Typically reserved for users who require District level access to batches, transactions, and downloads. This role can view the Location Administrator-DirectMatch, Building Administrator-DirectMatch and Building User- DirectMatch roles only. This user role typically does not have access to Security Manager or Configuration Manager or other system administrator functions. Formerly named District user - DirectMatch.	System Administrator - DirectMatch
CEP Manager	New Role: Typically reserved for users who will perform CEP Manager updates. This role typically only has access to CEP Manager functions and related Groups.	Location Administrator
Multiple Location – DirectMatch	New Role: Typically reserved for users who require access to batches, transactions, and downloads for multiple districts/locations within DirectMatch.	System Administrator

ROLE	DESCRIPTION	PARENT ROLE
	This user role typically does not have access to Security Manager or Configuration Manager or other system administrator functions. This role is managed by the LDOE.	

Role Profile

The Role Profile enables authorized users to configure the permissions and privileges for the selected role. The Role Profile includes a Profile Header, Details Tab and Privileges tab as described below. This page is accessed from the Security Manager Role Manager panel using the Drill In (») icon.

Role Profile Header

The Role Profile Header displays basic information about the selected role including the data below.

ROLE	DESCRIPTION
Role Name	Displays the full role name for the selected role.

ROLE	DESCRIPTION
Last Updated	Displays the date the role was last updated. A role is updated when any Details are edited, or Privileges are changed.

Role Details

The Details section displays more detailed information about the selected role including the data below.

ROLE	DESCRIPTION
General – Edit Icon	The Edit icon enables authorized users to edit the Role Status. No other fields are editable for system-generated roles. The Edit icon will only be visible to users with Role Manager Edit permissions.
Role Details – Role Name	Displays the full role name for the selected role.
Role Details – Description	Displays the role description name for the selected role.
Role Details – Status	Displays the status for the selected role. The options are Inactive or Active. If a role is inactive, no new users can be assigned to the role.
More – Last Updated	Displays the date the role was last updated. A role is updated when any Details are edited, or Privileges are changed.

ROLE	DESCRIPTION
More – Last Updated By	Displays the First and Last Name of the user who last updated the role. A role is updated when any Details are edited, or Privileges are changed.
More – Created	Displays the First and Last Name of the user who created the role.
More – Created By	Displays the date the role was created.

Privileges Tab

The Privileges Tab displays a Role Privilege Settings Panel which includes an Expand and a Collapse link button and listing of all permissions/privileges available in the application organized by category. The privileges are listed below.

i   Although the interface displays permissions for Person ID, these permissions will not be implemented in Version 2020.3. The Person ID permissions and functionality will be available in the 2021 release later this year.

Role Manager lists all the privileges that are available and when the Role Profile page is access, the Privileges Tab will be displayed in edit mode if the user has Role Manager -Edit privileges. The privilege option buttons will be clickable to enable or disable each privilege. If a user does not have the Role

Manager – Edit privilege, the Role Profile will be displayed in view mode. The following selection options are available for the privileges:

BUTTON	SYSTEM
☑	Indicates that the privilege is enabled.
☐	Indicates that the privilege is disabled.
No button/selector	Indicates that the privilege cannot be enabled/disabled. It is not available for the specified application.
☑	Indicates the privilege is enabled and cannot be edited by the user.

Application

PRIVILEGE	PERSON ID	DIRECTMATCH	LOCATION ID
Navigation - View	Not available in v2020.3, will be available in a future release.	If enabled, the users assigned to the role can access the DirectMatch component. The DirectMatch option will be available to the user from the Application Picker in the Main Header/Navigation Bar. This must be enabled if the users need to access any DirectMatch functions.	Not available

CEP Manager

CEP Manager

Privilege	Person ID	DirectMatch	Location ID
Approve Elections		☑	
Approve Population		☑	
CEP Manager - View		☑	
Recalculate Elections		☑	
Submit Elections		☑	
Submit Population		☑	

PRIVILEGE	PERSON ID	DIRECTMATCH	LOCATION ID
Approve Elections	N/A	If enabled, users assigned to the role can approve Elections data from the SFAs. Typically reserved for State-level roles with permissions to approve the Elections data submitted by SFAs.	N/A
Approve Population	N/A	If enabled, users assigned to the role can approve Populations data from the SFAs. Typically reserved for	N/A

PRIVILEGE	PERSON ID	DIRECTMATCH	LOCATION ID
		State-level roles with permissions to approve the Elections data submitted by SFAs.	
CEP Manager – View	N/A	If enabled, users assigned to the role can access the CEP Manager page by clicking the CEP Manager button on the side navigation bar. Typically reserved for SFA and State roles with permissions to view CEP data.	N/A
Recalculate Elections	N/A	If enabled, users assigned to the role can access the Recalculate Elections button on the Elections tab. Typically reserved for SFA roles with permissions adjust Elections data prior to submission.	N/A
Submit Elections	N/A	If enabled, users assigned to the role can submit the Elections data for their location(s). Typically reserved for SFA with permissions to submit CEP data.	N/A

PRIVILEGE	PERSON ID	DIRECTMATCH	LOCATION ID
Submit Population	N/A	If enabled, users assigned to the role can submit the Population data for their location(s). Typically reserved for SFA with permissions to submit CEP data.	N/A

Download

PRIVILEGE	PERSON ID	DIRECTMATCH	LOCATION ID
Download	Not available in v2020.3, will be available in a future release.	If enabled, users assigned to the role can download data from DirectMatch.	N/A

Match Processing

Privilege	Person ID	DirectMatch	Location ID
Delete Match Request		☑	
Edit Person	☑		
Fix Errors - Cancel	☑		
Fix Errors - Update	☑		
Fix Errors - View	☑		
Match History - View	☐	☐	☐
Match Options - Address Tab View		☐	
Match Options - Address Run Now		☐	
Match Options - Manual Match		☐	
Match Options - Individual Match	☑	☐	
Match Options - Person ID		☐	
Match Options - Person Tab View	☑	☐	
Match Options - Upload File	☑	☐	
Match Options - View	☑	☐	
Resolve Near Match - Assign Selected (SSN SAME)	☑		
Resolve Near Match - Cancel Record	☑	☐	☑
Resolve Near Match - Create ID (ID NOT PRESENT)	☑		
Resolve Near Match - Create ID (ID PRESENT)	☑		
Resolve Near Match - Create ID (SSN SAME)	☑		
Resolve Near Match - Match Decision	☑	☐	☑
Resolve Near Match - Match Decision (Assigns Existing ID)	☑	☐	
Resolve Near Match - No Match	☑	☐	☑
Resolve Near Match - No Match (Creates a New ID)	☑		☑
Resolve Near Match - Resolve Selected	☑	☐	☑
Resolve Near Matches - View	☑	☐	☑
State Match		☐	
Validate Data	☑	☐	

PRIVILEGE	PERSON ID	DIRECTMATCH	LOCATION ID
Delete Match Request	N/A	Not available in v2020.3, will be available in a future release.	N/A
Edit Person	Not available in v2020.3, will be available in a future release.	N/A	N/A
Fix Errors - Cancel	Not available in v2020.3, will be available in a future release.	N/A	N/A
Fix Errors – View	Not available in v2020.3, will be available in a future release.	N/A	N/A
Match History – View	If enabled, users assigned to the role can view the Match History page via the Dashboard.		

PRIVILEGE	PERSON ID	DIRECTMATCH	LOCATION ID
Match Options – Address Tab	N/A	If enabled, users assigned to the role can access the Match Options – Address tab to view address matches.	N/A
Match Options – Address Run Now	N/A	If enabled, users assigned to the role can run an Address match. This is limited to State-level roles/users.	N/A
Match Options – Manual Match	N/A	If enabled, users assigned to the role can add, edit, and delete Manual Matches from the Match Options – Manual Match page. This is dependent on the Match	N/A

PRIVILEGE	PERSON ID	DIRECTMATCH	LOCATION ID
		Options – Person Tab privilege.	
Match Options – Individual Match	Not available in v2020.3, will be available in a future release.	If enabled, users assigned to the role can submit a match request for an individual record from the Match Options – Individual page from within DirectMatch. This is dependent on the Match Options – Person Tab privilege.	N/A
Match Options – Person ID	N/A	If enabled, users assigned to the role can submit Person ID matches. This is dependent on the Match	N/A

PRIVILEGE	PERSON ID	DIRECTMATCH	LOCATION ID
		Options – Person Tab privilege.	
Match Options – Person Tab	Not available in v2020.3, will be available in a future release.	If enabled, users assigned to the role can view the Person Tab within the Match Options feature. This is dependent on the Match Options – View privilege.	N/A
Match Options – Upload File	Not available in v2020.3, will be available in a future release.	If enabled, users assigned to the role can upload a file for matching from the Match Options feature. This is dependent on the Match Options – Person Tab privilege.	N/A

PRIVILEGE	PERSON ID	DIRECTMATCH	LOCATION ID
Match Options – View	Not available in v2020.3, will be available in a future release.	If enabled, users assigned to the role can view the Match Options icon ( ) in the Side Navigation and to access the Match Options functions. The other Match Options appropriate for the role should also be enabled.	N/A
Resolve Near Match – Assign Selected (SSN Same)	Not available in v2020.3, will be available in a future release.	N/A	N/A
Resolve Near Match – Cancel Record	Not available in v2020.3, will be available in a future release.	If enabled, users assigned to the role can cancel a pending Near Match using the Cancel Submission link	N/A

PRIVILEGE	PERSON ID	DIRECTMATCH	LOCATION ID
		on Compare Records pages within DirectMatch.	
Resolve Near Match – Create ID (ID Not Present)	Not available in v2020.3, will be available in a future release.	N/A	N/A
Resolve Near Match – Create ID (ID Present)	Not available in v2020.3, will be available in a future release.	N/A	N/A
Resolve Near Match – Create ID (SSN Same)	Not available in v2020.3, will be available in a future release.	N/A	N/A
Resolve Near Match – Match Decision	Not available in v2020.3, will be available in a future release.	If enabled, users assigned to the role can select "Match" (Assign ID) on the Near Match List and	

PRIVILEGE	PERSON ID	DIRECTMATCH	LOCATION ID
		Compare Records pages within DirectMatch.	
Resolve Near Match – Match Decision (Assigns Existing ID)	Not available in v2020.3, will be available in a future release.	N/A	N/A
Resolve Near Match – No Match	Not available in v2020.3, will be available in a future release.	If enabled, users assigned to the role can select "No Match" on the Near Match List and Compare Records pages within DirectMatch.	N/A
Resolve Near Match – No Match (Creates New ID)	Not available in v2020.3, will be available in a future release.	N/A	N/A

PRIVILEGE	PERSON ID	DIRECTMATCH	LOCATION ID
Resolve Near Match – Resolve Selected	Not available in v2020.3, will be available in a future release.	N/A	
Resolve Near Match – View	Not available in v2020.3, will be available in a future release.	If enabled, users assigned to the role can view Near Matches.	
State Match	N/A	If enabled, users assigned to the role can run a State Match.	N/A
Validate Data	Not available in v2020.3, will be available in a future release.		

Person Profile

PRIVILEGE	PERSON ID	DIRECTMATCH	LOCATION ID
Person Profile – View	Not available in v2020.3, will be available in a future release.	If enabled, users assigned to the role can view the Person Profile page.	N/A

Other

These privileges are limited to State users only.

PRIVILEGE	PERSON ID	DIRECTMATCH	LOCATION ID
View – State Views	N/A	Not available	N/A

Reports

PRIVILEGE	PERSON ID	DIRECTMATCH	LOCATION ID
Canceled Record Report	Not available in v2020.3, will be available in a future release.	N/A	N/A
FNS 834	N/A	If enabled, users assigned to the role can access and download this report.	N/A
Locations Serving only NSLP with High ISP	N/A	If enabled, users assigned to the role can access and download this report. This report is intended for State-level roles only.	N/A
May Report to USDA	N/A	If enabled, users assigned to the role can access and download this report. This	N/A

PRIVILEGE	PERSON ID	DIRECTMATCH	LOCATION ID
		report is intended for State-level roles only.	
Near Match Report	Not available in v2020.3, will be available in a future release.	N/A	N/A
No History Report	Not available in v2020.3, will be available in a future release.	N/A	N/A
Reports – View	Not available in v2020.3, will be available in a future release.	If enabled, users assigned to the role can access the Reports feature and the Reports icon () will be available on the Side Navigation bar.	

PRIVILEGE	PERSON ID	DIRECTMATCH	LOCATION ID
September Report to USDA	N/A	If enabled, users assigned to the role can access and download this report. This report is intended for State-level roles only.	N/A
Submission History Report	Not available in v2020.3, will be available in a future release.	N/A	N/A

Searching

Searching

Privilege	Person ID	DirectMatch	Location ID
Search Options - Add Person from Search	☑		
Search Options - Batch Search	☑		
Search Options - Person Search	☑	☐	
Search Options - Search Input Record	☑		
Search Options - Search SSN	☑		
Search Options - View	☑	☐	☑

PRIVILEGE	PERSON ID	DIRECTMATCH	LOCATION ID
Search Options – Add Person from Search	Not available in v2020.3, will be available in a future release.	N/A	N/A
Search Options – Batch Search	Not available in v2020.3, will be available in a future release.	N/A	N/A

PRIVILEGE	PERSON ID	DIRECTMATCH	LOCATION ID
Search Options – Person Search	Not available in v2020.3, will be available in a future release.	If enabled, users assigned to the role can perform a search from the Search Options – Person Search page.	N/A
Search Options – Search Input Record	Not available in v2020.3, will be available in a future release.	N/A	N/A
Search Options – Search SSN	Not available in v2020.3, will be available in a future release.	N/A	N/A
Search Options – View	Not available in v2020.3, will be available in a future release.	If enabled, users assigned to the role can access the Search Options feature and the Search icon ( ) will	

PRIVILEGE	PERSON ID	DIRECTMATCH	LOCATION ID
		be available on the Side Navigation bar.	

Security

PRIVILEGE	SYSTEM
Role Manager – Edit Role	If enabled, users assigned to the role can edit a role configuration including the status and privileges assigned to the role. This permission is restricted to System

PRIVILEGE	SYSTEM
	Administrators, but if enabled users can only edit roles below their own role. This permission is dependent on the Role Manager – View permission.
Role Manager – View	If enabled, users assigned to the role can view the Role Manager panel within Security Manager.
Security Manager - View	If enabled, users assigned to the role can view the Security Manager feature and the Security Manager icon () will be available on the Side Navigation bar.
User Manager – Add	If enabled, users assigned to the role can add a user to the application. This permission should be restricted to System Administrators, but if enabled users can only add users based on data authorization rules. For example, a Location Administrator who is restricted to Happyville District, can only add users for Happyville. This permission is dependent on the User Manager – View permission.
User Manager – Edit	If enabled, users assigned to the role can edit a user to the application. This permission should be restricted to System Administrators, but if enabled users can only edit users based on data authorization rules. For example, a Location Administrator

PRIVILEGE	SYSTEM
	who is restricted to Happyville District, can only edit users for Happyville. This permission is dependent on the User Manager – View permission.
User Manager – Reset Password	If enabled, users assigned to the role can initiate the password reset process. This permission is dependent on the User Manager – View permission.
User Manager – View	If enabled, users assigned to the role can view User Manager within Security Manager. This permission should be restricted to System Administrators, but if enabled users can only view users based on data authorization rules. For example, a Location Administrator who is restricted to Happyville District, can only view users for Happyville. This permission is dependent on the Security Manager – View permission.

System Management

These previleges are limited to State users.

Lesson: How to View a Role Profile

1. Navigate to the Security Manager component by clicking the Security Manager icon ( ) on the Side Navigation bar.

2. The application will display the Security Manager landing page with the User Manager and Role Manager panels.

3. Identify the role to be viewed.

4. Click the Drill Into ( ) icon to navigate to the Role Profile for the selected role.

5. The application will navigate to the Role Profile and will display the Privileges tab by default.

    a. Review the privilege settings as needed.

6. Click on the Details tab to view the Role Profile details such as status and last update date.

◾ **Security Manager - User Manager**

The User Manager component provides authorized users with a view of the users registered in the application and to perform actions such as add a user, edit a user, and reset a password. User Manager includes a count of user, Add Records button, User List Filter, and a User List.

When a user accesses User Manager, the list of users will be dependent on the data authorization of the user. For example, if a Location Administrator for Happyville accesses User Manager, this user can only view Happyville users. Additionally, users can only view other users at or below their own role level. For example, a Happyville Location Administrator cannot view or edit a State Administrator.

Add Records

The Add Records button enables authorized users to register/invite new users to the application. When clicked, the Add Records button will navigate the user to the Add Options – User page, which includes a form for submitting new users.

The form includes the following:

OPTION	DESCRIPTION
Person Information – First Name	Identifies the full First Name of the user to be added. The value entered here will be displayed in the Main Header / Navigation bar for the user when they are logged in. The text field allows up to 60 characters and is required.
Person Information – Last Name	Identifies the full Last Name of the user to be added. The value entered here will be displayed in the Main Header / Navigation bar for the user when they are logged in. The text field allows up to 60 characters and is required.

Login Information - Email	Identifies the email address of the user to be added. This email address will be used for account setup and all other alerts/communications from the application and it also serves as the username. The text field allows up to 60 characters and is required.
Authorization Information – Role	Identifies the role to be assigned to the new user. The drop-down menu will list all active roles that are available to the administrator and a search option. The administrator adding the new user only has access to roles at or below their own role level. For example, a Location Administrator cannot add a user to a System Administrator role.
District	This button group field option is only available if the selected role has access to Person ID and/or DirectMatch and may include:

Option	Description
All Districts	If the administrator creating the new user has access to All Districts in the application, this button will be available. If selected, the new user will be able to access data for all Districts in the application.
Specific District	If the administrator creating the new user has access to one or many Districts, this button option will be displayed. When clicked a District Picker menu will be displayed in the District(s) field below and will list all the

	districts the administrator has access to in the application.
District(s)	Identifies the District(s) to be assigned to the new user. This is the primary indication of what data, batches, transactions and near matches the user can access in the system. This selection is important to security of the data and student records and should be limited to the specific locations the user is authorized to access. The view will vary by administrator because it is based on the data the administrator is able to access. For example, a Location Administrator for Happyville will not be able to view/select Sleepyville.
	This District Picker menu will display a search box and a listing of up to 25 Districts that the administrator has access to in the application. One or many locations can be selected, if available.
	The District Picker menu includes the District Name and District Code for each available options. The search must

	be used to filter the list if more than 25 options are available.
School	This button group field option is only available if the selected role has access to Person ID and/or DirectMatch and may include:
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>All Schools</td><td>If the administrator creating the new user has access to All Schools with the selected district(s) in the application, this button will be available. If selected, the new user will be able to access data for all Schools within the selected Districts in the application.</td></tr><tr><td>Specific School</td><td>If the administrator creating the new user has access to one or many Schools, this button option will be displayed. When clicked a School Picker menu will be displayed in the School(s) field below and will list all the schools the administrator has access to in the application.</td></tr></table>
Schools(s)	Identifies the Schools(s) to be assigned to the new user. This is the primary indication of what data, batches, transactions and near matches the user can access in the system. This selection is important to security of the data

	and student records and should be limited to the specific locations the user is authorized to access. The view will vary by administrator because it is based on the data the administrator is able to access. For example, a Location Administrator for Happyville will not be able to view/select Sleepyville.
	This School Picker menu will display a search box and a listing of up to 25 Districts that are associated to the selected District(s) and that the administrator has access to in the application. One or many schools can be selected, if available.
	The School Picker menu includes the Location ID, School Name, School Code, District Name and District Code for each available options. The search must be used to filter the list if more than 25 options are available.
DirectMatch Type(s)	Identifies the Match Type to be assigned to the new user. This is the primary indication of what Match Types the user can select on the Match Options pages. For example, if SNAP is the only Match Type enabled for a role, users in that role will only be able to select SNAP on the Match Options – Upload File page.
	This drop-down menu lists all the Match Types the active Match Types and based on the data the administrator can access, as long as the user has access to the DirectMatch module with DirectMatch Navigation View permissions. For example, an administrator with access to only SNAP and TANF cannot add Foster to another user.

	DirectMatch Match Type(s) _____ ☐ Foster ☐ SNAP Location Group ☐ TANF *If this user needs additional role assignments, ple...* Clear *...ser.*
Location Group	This button group field option is only available if the selected role has access to DirectMatch and/or Location ID and may include: 	Option	Description	 |---|---| 	All Groups	If the administrator creating the new user has access to All Groups in the application, this button will be available. If selected, the new user will be able to access data for all Location Groups.	 	Specific Groups	If the administrator creating the new user has access to one or many groups, this button option will be displayed. When clicked a Location Group Picker menu will be displayed in the Location Group(s) field below and will list all the groups the administrator has access to in the application.	 This selection is particularly important for CEP Manager. For a user to view SFA information in CEP Manager, an SFA Group must be assigned to the user in Location Groups.

Location Group(s)	Identifies the Location Groups to be assigned to the new user. This is the primary indication of what locations the user can access in Location ID and/or in Direct Match, specifically CEP Manager.
	This drop-down menu lists all the Location Groups based on the data the administrator can access. For example, an administrator with access to 5 Location Groups will only view those 5 Location Groups in this list. An administrator cannot assign a Location Group to a new user if they do not have access to the group themselves.

Lesson: How to Add a User

1. Click on the Security Manager icon ( ) on the Side Navigation bar.

    a. User must have the Security Manager – View privilege and the User Manager – Add permission to add User.

2. Click the Add User icon ( ) in the upper right corner of the User Manager panel.

3. The application will display the Add Options form in add mode.

4. Enter the First Name, Last Name, and Email of the user.

5. Select the primary role from the dropdown list. Refer to the Roles and Privileges above.

   a. The application allows one user to have multiple roles, but the user must have a primary role.

   b. If the selected role does not have permission to Person ID and/or DirectMatch, some fields below will not be available.

6. Once a role is selected the application will dynamically display the allowable options for the role and based on Data Authorization for the administrator entering the new user.

    a. If the administrator does not have access to a district, school, or group, those options will not be available in the form. This prevents a user from adding a new user with more privileges or data access than their own account.

7. Select the appropriate District button option.

    a. If the user to be added requires access to all districts, click All Districts button option, if available. Note: Not all options will be available depending on data access.

    b. If the user to be added requires access to one or many districts, click the Specific Districts button option.

8. If Specific Districts was selected in the previous step, the application will display the allowable options in the Districts(s) section.

9. Click on the District Picker drop-down menu.

10. The application will dynamically display the first 25 allowable District options based on Data Authorization for the administrator entering the new user.

    a. If the District is not listed, perform a search by entering at least 3 letters of the District Name into the District Picker search bar.
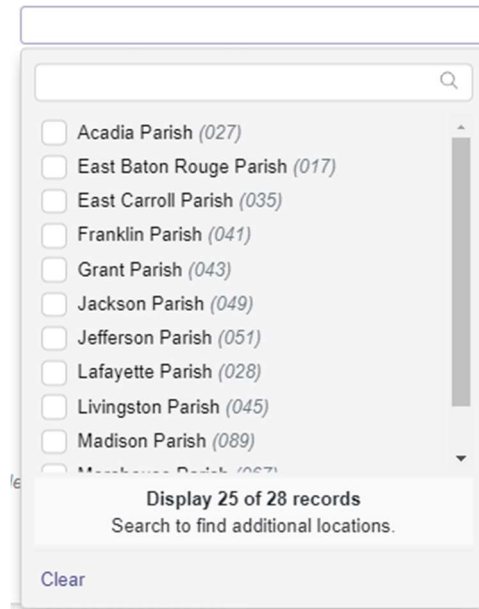
11. Select/Check each District to be granted to the new user.

12. The application will display the selected Districts in the District(s) field. Each selected District will be listed with the District Name, District Code, and an "x".

District(s)

| Acadia Parish (027) × | East Carroll Parish (035) × |
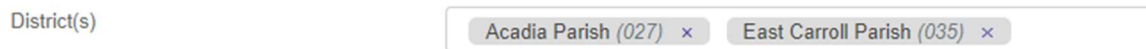
    a. To remove a District from the District(s) list, click the "x" to the right of the District Name.

13. Select the appropriate School button option.

    a. If the user to be added requires access to all schools for the School(s) selected in the previous step, click All Schools button option, if available. Note: Not all options will be available depending on data access.
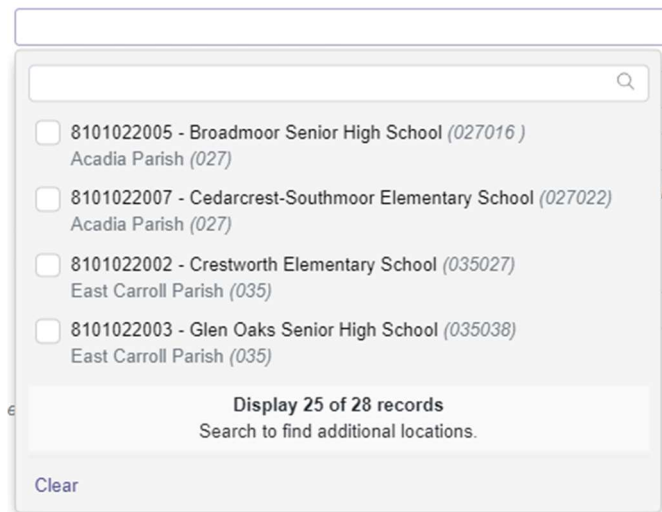
    b. If the user to be added requires access to one or many schools, but not all schools, click the Specific Schools button option.

14. If Specific Schools was selected in the previous step, the application will display the allowable options in the School(s) section.

15. Click on the School Picker drop-down menu.

16. The application will dynamically display the first 25 allowable School options based on Data Authorization for the administrator entering the new user. The list will only include Schools that are associated to the selected District.

    a. If the School is not listed, perform a search by entering at least 3 letters of the School Name into the School Picker search bar.

17. Select/Check each Schools to be granted to the new user.

18. The application will display the selected Schools in the School(s) field. Each selected School will be listed with the Location ID, School Name, School Code, and an "x".

19. Select DirectMatch Match Type(s) from the Match Type selector.

    a. If the administrator does not have access to a Match Type, the Match Type option will not be available in the form. This prevents a user from adding a new user with more privileges or data access than their own account.

20. The application will display the selected Match Types in the Match Type(s) field. Each selected Match Type will be listed with the Match Type Name and an "x".

21. Select the appropriate Location Group button option.

    a. If the user to be added requires access to all Location Groups, click All Location Groups button option, if available. Note: Not all options will be available depending on data access.

    b. If the user to be added requires access to one or many Location Groups, click the Specific Location Group button option.

The Location Group selection determines which Location Groups the user can access in Location ID and CEP Manager. If the new user being added will be responsible for CEP Manager, it is important to select the correct SFA / FNS Location Group for the user. This group selection will determine which SFA the user has access to in CEP Manager.

---

22. The application will display the selected Location Groups in the Location Group(s) field. Each selected Location Group will be listed with the Group Name and an "x".

23. Click the Add User icon to submit the new user.

Add User

24. The application will perform form validation and either accept or reject the submission.

a. If the form is rejected due to a validation issue, the application will display an error at the top of the page and below the field in the error state.

⊘ There were some errors. Please fix the errors highlighted in the fields below.

First Name is required.

Last Name is required.

sample@email.com
Email address is required.
Email address is used as username.

b. If the form is accepted with no validation errors, a success message will be displayed at the top of the page and the Security Manager landing page will be displayed.

✔ The user has been added successfully.
✔ Account Sign-up email has been sent to the user.

25. The newly created account will remain in a Pending status until the user completes the set-up process.

User List Filter Options

The User List Filter Options section include a Filter Options button to expand or collapse the filter options.

OPTION	DESCRIPTION
Email or Last Name	Enables a filter to be applied for an email address or Last Name of the user.
Role	Enables a filter by role name. The valid options will be available in the drop-down menu.
Account Status	Enables a filter by Account Status for Active, Inactive or Pending statuses. The valid options will be available in the drop-down menu.
Log In Status	Enables a filter for all users or only the users currently logged into the application. To filter on the logged in users only, the checkbox must be clicked.
District	Enables the selection of one or many Districts. The valid options will be displayed in a multiple select drop-down menu. This drop-down also allows for searching. By default, the list will only include the top 25 locations.

School	Enables the selection of one or many Schools. The valid options will be displayed in a multiple select drop-down menu. This drop-down also allows for searching. By default, the list will only include the top 25 locations.
Location Group	Enables the selection of one or many Location Groups. The valid options will be displayed in a multiple select drop-down menu. This drop-down also allows for searching. By default, the list will only include the top 25 groups.

User List

The User List includes a list of all the users in the application, sorted by Last Update Date. The list of users will be limited based on the Data Authorization rules. For instance, a Location Administrator for Happyville cannot view users for Sleepyville. Additionally, users can only view roles at or below their own role. For instances, a Location Administrator cannot edit/view a Super User account.

FIELD	DESCRIPTION

Email	Displays the email address for the user.
First Name	Displays the full First Name for the user.
Last Name	Displays the full Last Name for the user.
Status	Displays the account status for the user. The options are: 	Status	Description	 |---|---| 	Pending	The account was added by a System Administrator, but the user has not finished the set-up process.	 	Active	The account is set up and can be accessed by the user.	 	Inactive	The account is locked and cannot be accessed by the user.	
Last Login	Displays the date and time the user last logged into the application.
Role	Displays the roles the user is assigned to in the application.
Actions	The Actions available in the User List are: 	Action	Description	 	---	---	 	🔑	Force Password Change: Initiates a "Force Password Change" process. This requires the user to change their password the next time	

		they log into the system. If a user needs to change their password without logging in, the forgot password process should be used from the Login page.
	🗑	Delete: Initiates the Delete User process. This is only available if the Account Status is Pending.
	✈	Resend: Initiates the Resend Account Set Up process to the user. When clicked, the application will send an Account Set Up email to the user with a link to complete the process.
	»	Drill Into: Navigates to the User Profile when clicked.

User Manager — 10 Users — Add Records

Filter Options ⌃

Email ⇕	First Name ⇕	Last Name ⇕	Status ⇕	Last Login ⇕	Role	Actions
ahartman@escholar.com	Andrea	Hartman	Active	05/28/2019	Location Administrator Super	🔑 »
nmoideen@escholar.com	Nishan	Moideen	Inactive	05/10/2019	Super	»
yzhang@escholar.com	Yuqing	Zhang	Pending		Help Desk	🗑 ✈ »
nmoideen@escholar.com	Nishan	Moideen	Active	05/10/2019	System Administrator	🔑 »
ahartman@escholar.com	Andrea	Hartman	Active	05/28/2019	Building Administrator	🔑 »
nmoideen@escholar.com	Nishan	Moideen	Active	05/10/2019	Building User	🔑 »
ahartman@escholar.com	Andrea	Hartman	Active	05/28/2019	Building User - DirectMatch	🔑 »
nmoideen@escholar.com	Nishan	Moideen	Active	05/10/2019	Location Administrator	🔑 »
ahartman@escholar.com	Andrea	Hartman	Active	05/28/2019	Super	🔑 »
nmoideen@escholar.com	Nishan	Moideen	Active	05/10/2019	Location Administrator - Location ID	🔑 »

1 - 10 of 10   Previous **1** Next

Lesson: How to Filter the User List

1. Click on the Security Manager icon ( ) on the Side Navigation bar.

2. Click on the Filter button on the top right of the User Manager panel to expand the filter options.

Filter Options ⌃

3. Enter/Select filter values as described above.

    a. For example, to filter the User List based on the Account Status, select the appropriate Account Status from the filter list.

4. Click the Filter Data button to submit the filter options.

    a. To reset the form, click the Reset link.

Reset   **Filter Data**

5. The application will apply the filters and update the User List data grid.

Lesson: How to Resend Sign-Up Email to a Pending User

1. Click on the Security Manager icon ( ) on the Side Navigation bar.

2. On the User Manager panel, click the Resend icon ( ) next to the pending email address (username).

3. The application will display a success message at the top of page and will send an email to the user to continue the set-up process.

✔ Account Sign-up email has been sent to the user.

Lesson: How to Reset a User's Password

1. Click on the Security Manager icon ( ) on the Side Navigation bar.

2. On the User Manager panel, click the Reset Password icon ( ) next to the pending email address (username).

3. The application will display a success message at the top of page and will require the user to reset their password the next time the user logs in.

✔ Reset password is done.

ℹ️ This process does not reset the password for the user. Rather it requires the user to change their own password the next time the user logs into the application. A user must use the reset password option from the log in page to reset their own password.

Lesson: How to Delete a Pending User

1. Click on the Security Manager icon ( ) on the Side Navigation bar.

2. On the User Manager panel, click the Delete icon ( ) next to the pending email address (username).

3. The application will display a confirmation modal requiring the user to confirm the deletion.

    a. Deleted users cannot be recovered.
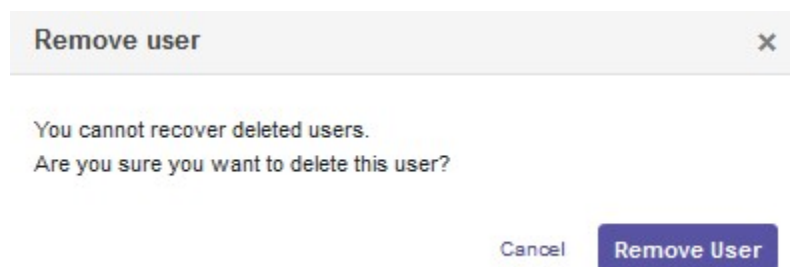
4. Click Remove User to permanently delete the account from the application.

5. The application will display a success message at the top of the screen stating that the pending user has been deleted.

◼ User Profile

The User Profile serves as a comprehensive profile for the user, including a Profile Header, General Information, Authorization Information, and Security Information panels. The primary purpose of the User Profile is to view and configure role and data authorization. The details of each panel are provided below.

Access to the User Profile is controlled by the User Manager – View privilege and edit privileges of a profile are controlled by the User Manager - Edit privilege.

General
View/edit general profile information ✎

Personal Details

First Name	Andrea
Middle Name	
Last Name	Hartman
Date of Birth	10/23/2001
Gender	female
Email	▓▓▓▓▓
Phone 1	(555) 555-5555
Phone 2	(555) 999-9999
Title	Superintendent

Address Details

Address 1	15990 Bloomingdale Ave
Address 2	
City	White Plains
State	New York
Zip	10605-0543

More

Status	Active
Last Updated	04/29/2019

Details: General

Authorization Information +

Location Administrator ✎ 🗑

Role	Location Administrator
District	Specific Districts
District(s)	Acadia Parish (027)
School	Specific Schools
School(s)	Broadmoor Senior High School (027016) Cedarcrest-Southmoor Elementary School (027022)
Person Type(s)	Staff
DirectMatch Match Type(s)	SNAP
Location Group	Specific Groups
Location Group(s)	00001 – Accountability Group

Details: Authentication Info

Security
View login and reset password. Reset Password

Log In Information

Email Address (User Name)	▓▓▓▓▓
Last Log In	08/06/2019 15:28 PM
Last Password Change	05/02/2019 09:10 AM

Details: Security Info

47

Profile Header

FIELD	DESCRIPTION
Name	Displays the First and Last Name of the selected user.
Email	Displays the email address for the selected user.
Phone	Displays the phone number, if available, for the selected user.
Status	Displays the Account Status for the selected user. The valid options are Active, Inactive or Pending.
Last Login	Displays the date the user last logged in to the application.
Last Updated	Displays the date account information was updated for the selected user. This could include changes in General Information, Authorization Information or Security Information.

General Panel

The General Panel displays information about the user as described below and includes an Edit icon ( ) if the permission is enabled for the person viewing the User Profile.

When the Edit icon is clicked, the application displays the General Panel data in an edit mode form. All fields are editable except the Email Address and Last Updated Date fields.

The fields available in the General Panel are:

SECTION	FIELD	DESCRIPTION
Person Details	First Name	Displays the First Name of the selected user.
	Middle Name	Displays the Middle Name, if available, of the selected user.
	Last Name Date of Birth	Displays the Date of Birth of the selected user.
	Gender	Displays the Gender, if available, of the selected user.
	Email	Displays the email address of the selected user.
	Phone 1	Displays the Phone 1, if available, of the selected user.
	Phone 2	Displays the Phone 2, if available, of the selected user.

	Title	Displays the Title, if available, of the selected user.
Address Details	Address 1	Displays the Address 1, if available, of the selected user.
	Address 2	Displays the Address 2, if available, of the selected user.
	City	Displays the City, if available, of the selected user.
	State	Displays the State, if available, of the selected user.
	Zip	Displays the Zip, if available, of the selected user.
More	Status	Displays the Account Status for the selected user. The valid options are Active, Inactive or Pending.
	Last Updated	Displays the date account information was updated for the selected user. This could include changes in General Information, Authorization Information or Security Information.

Authorization Information

The Authorization Information panel displays the information about the data and features the user will have access to in the application.

The Authorization Information panel includes an Add icon (+) and a listing of each role assigned to a user. Most users will have one role, but one user can have more than one role, allowing different permissions per location if needed. If a user is given two roles within the same location, the sum of the privileges will be used.

The role information will be displayed in View mode unless the Edit icon (✎) is clicked. When in edit mode, the form has the same options and selections available as the Add Record and Add a Role pages.

FIELD	DESCRIPTION
Role Title	Identifies the role for the user and serves as a header for the other role details. It includes the following: 	Option	Description	 	✎	Edit: If available, the Edit icon enables authorized user to edit the details of the specific role for the user.	 	🗑	Delete: If available, the Delete icon enables authorized users to delete the specific role. There must be at least one role assigned to the user.	
Role	Identifies the role for the user.
District	This field option is only available if the selected role has access to Person ID and/or DirectMatch and may include an All Districts or Specific Districts label.
District(s)	Identifies the District(s) assigned to the user. This is the primary indication of what data, batches,

	transactions and near matches the user can access in the system.
	The field includes the District Name and District Code for each assigned location.
School	This field is only available if the selected role has access to Person ID and/or DirectMatch and may include an All Schools or Specific Schools label.
Schools(s)	Identifies the Schools(s) assigned to the user. This is the primary indication of what data, batches, transactions and near matches the user can access in the system.
	This field includes the Location ID, School Name, School Code, District Name and District Code for each available option.
DirectMatch Match Type(s)	Identifies the Match Type(s) assigned to the new user. This is the primary indication of what Match Types the user can select on the Match Options pages. For example, if SNAP is the only Match Type enabled for a role, users in that role will only be able to select SNAP on the Match Options – Upload File page.
Location Group	This field is only available if the selected role has access to DirectMatch and/or Location ID and may include an All Groups or Specific Groups label.
	This selection is particularly important for CEP Manager. For a user to view SFA information in CEP

	Manager, an SFA Group must be assigned to the user in Location Groups.
Location Group(s)	Identifies the Location Groups assigned to the user. This is the primary indication of what locations the user can access in Location ID and/or in Direct Match, specifically CEP Manager.

Security Panel

The Security Panel includes Log In information for the user, including the following:

FIELD/OPTION	DESCRIPTION
Reset Password	If an authorized user is viewing a User Profile for another user, the Reset Password link will be available. It will initiate the Reset Password for the user.
Edit	If an authorized user is viewing their own User Profile, an Edit icon ( ) will be displayed. When clicked the Security Information section will be displayed in edit mode.
Email Address (User Name)	Indicates the email address of the user. This also serves as the user name.
Last Log In	Indicates the date the user last logged into the application.

Last Password Change	Indicates the date the user last changed their password.

If the Edit icon ( ) is clicked on the Security Information panel, the application will display the information in Edit mode. The administrator will be able to update the password.

Lesson: How to View a User Profile

1. Click on the Security Manager icon ( ) on the Side Navigation bar.

    a. User must have the "User Manager – View" permission to view User profile.

2. On the User Manager panel, click the email address or the Drill In icon ( ) for the user profile to be viewed.

3. The application will display the User Profile for the selected user.

4. View the User Profile as needed.

Lesson: How to Edit the User Profile – General

1. Follow steps 1-4 in Lesson: How to View a User Profile above.

    a. User must have the "User Manager – Edit" permission to edit a User Profile.

2. To edit the General details, click Edit icon ( ) in the General Panel header.

3. The application will display the User Profile – General Information in edit mode.

4. Edit the First Name, Middle Name, Last Name, Date of Birth, Gender, Phone Numbers, Title, Address, and/or the Status of the User.

5. Click the Update button to save changes to the General data.

    a. Click the Cancel link to cancel the changes.

6. The application will return to the User Profile in view mode.

Lesson: How to Edit the Role

1. Follow steps 1-4 in Lesson: How to View a User Profile above.

    a. User must have the "User Manager – Edit" permission to edit a User Profile.

2. Edit the District, School, Match Type and/or Location Group of the role for User. The edit rules are the same as the add user and add role processes.

7. Click the Update button to save changes to the General data.

    b. Click the Cancel link to cancel the changes.

8. The application will save the changes and then return to the User Profile in view mode.

Lesson: How to Add the Role to user

1. Follow steps 1-4 in Lesson: How to View a User Profile above.

    a. User must have the "User Manager – Edit" permission to edit a User Profile.

2. Click the Add icon (+) in the Authorization Information panel to add a new role to the user.

3. The application will display a new section with an Add Role form.

4. Select the secondary role / new role to add to the user.

5. Based on the role selection, the form will be dynamic. This is the same as the add user process described above.

6. Select/Enter the District, School, Match Type and/or Location Group of the role for User.

7. Click the Add Role button to add the new role.

   a. Click the Cancel link to cancel the changes.

8. The application will insert the new role and then return to the User Profile in view mode.
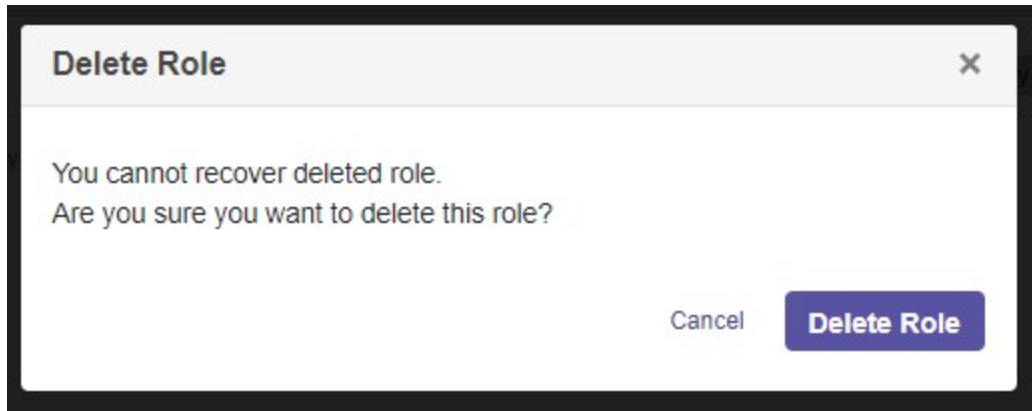
Lesson: How to Delete the Role from user

1. Follow steps 1-4 in Lesson: How to View a User Profile above.

   a. User must have the "User Manager – Edit" permission to edit a User Profile.

2. If the user has more than one role, the Delete icon (🗑) to the right of the role name. If the Delete icon is disabled, the role cannot be deleted.

3. To delete a role, click Delete icon (🗑) in the role header.

4. The application will display a Delete Role prompt with a Cancel link and a Delete Role button.

5. Confirm the deletion by clicking the Delete Role button.

6. The application will display a success message at the top of the page and will return to view mode for the User Profile.

Lesson: How to Reset a Password

1. Follow steps 1-4 in Lesson: How to View a User Profile above.

   a. User must have the "User Manager – Reset Password" permission to initiate the reset password process in a User Profile.

2. From the User List, click the Reset Password icon ( ). From the User Profile, click the Reset Password link in the Security panel.

3. A message will appear at the top of the screen and it will force the user to reset password next time when they login.

   a. To cancel the updates, click the Cancel link.

◾ **Appendix A: Documentation**

Documentation for eScholar Uniq-ID® is provided for end user and administrative functions. The information below describes each document.

DirectMatch User Guide

The DirectMatch User Guide provides overview information for each feature and instructions for functions within the application. This document describes the non-administrator functions that a typical user might need to understand.

Administrator Guide: Security Management

The Administrator Guide: Security Management documentation provides overview information for security-related topics and detailed information about Security Manager – User Manager, Security Manager – Role Manager, and the User Profile. This guide is meant for administrative users who will be managing users and other security settings. Typical end users should not have access to these capabilities because they can impact the entire system.